UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/696,584	10/24/2000	Ryuichi Iwamura	SONY-50P4042.US.P	3340

7590   12/30/2004

Wagner Murabito & Hao LLP
Two North Market Street
Third floor
San Jose, CA 95113

EXAMINER
DADA, BEEMNET W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
    application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1, 6, 14,15 and 24 have been amended on an amendment filed on July 26, 2004.

Claims 1-25 are pending.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.   Claims 1 and 6 are rejected under 35 U.S.C. 102(e) as being anticipated by Ciacelli et

al. US Patent 6,236,727 (hereinafter Ciacelli).

4.   As per claim 1, Ciacelli teaches a method of processing a digital signal comprising the

steps of:

        receiving encrypted signal at a first logical circuit of a device (i.e., receiving encrypted

data at module 23 or device 27) [column 6, lines 23-25];

determining a broadcast encryption key for said encrypted signal at a first location within

said device separate from said first logical circuit (encryption key is generated within module 22,

for encrypting the data) [column 6, lines 34-45] ;

encrypting said broadcast encryption key at said first location [column 6, lines 40-41];

transferring said encrypted broadcast encryption key to said first logical circuit over a

communication link [column 6, lines 42-45];

at said first logical circuit, decrypting said encrypted broadcast encryption key to

determine said broadcast encryption key [column 6, lines 45-52]; and

at said first logical circuit, decrypting said encrypted signal using said broadcast

encryption key [column 6, lines 45-53].

5.   As per claim 6, Ciacelli teaches the method as applied above. Furthermore, Ciacelli

teaches the method wherein said encrypted signal is substantially compliant with a Motion

Pictures Experts Group (MPEG) format [column 3, lines 40-43].

6.   Claims 10-11 are rejected under 35 U.S.C. 102(b) as being anticipated by Iijima US

Patent 5,202,922.

7.   As per claim 10, Iijima teaches a method of processing a digital signal comprising the

steps of:

generating a local encryption key (generating a data key in random generator unit 206)

[column 3, lines 33-36, figure 2] ;

transferring said local encryption key across a communication link to a first logical circuit

and to a second logical circuit (transferring the encryption key to IC card 1 and to encryption

section within host device 2) [column 3, lines 33-48];

with said local encryption key, encrypting said digital signal at said first logical circuit

[column 3, lines 53-61];

transferring said digital signal to said second logical circuit [column 3, lines 53-61]; and

using said local encryption key, decrypting said digital signal at said second logical

circuit, wherein said digital signal is transferred from said first logical circuit to said second

logical circuit in an encrypted form [column 3, lines 65-67].

8.   As per claim 11, Iijima teaches the method as applied above. Furthermore, Iijima

teaches before transferring local encryption key across a communication link encrypting said

local encryption key [column 3, lines 39-42].

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10.   Claims 19-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold

et al, US Patent 6,668,324, in view of Iijima US Patent 5,202,922, and further in view of Nally et

al, US Patent 5,808,629.

11.   As per claim 19, Mangold et al discloses a first logical circuit (see for example, PCX

module; col 6 In 31-65 and 106 of fig 1) comprising a local encryptor (see for example; PCX

encryptor, col 6 In 31-42 and fig 4) and a second logical circuit (see for example; video decoder,

col 6 In 31-64) comprising a local decryptor (see for example; video decoder decrypts, col 6 In

56-64), said local decryptor operable to decrypt a signal encrypted with said local encryptor (see

for example, col 6 In 31-64).

As for, the first logical circuit operable to decrypt a first local key using a first value

stored in said first hidden register; and said second logical circuit operable to decrypt a second

local key using a second value stored in said second hidden register, Mangold discloses a

means of key exchange for obtaining such keys (see for example, col 6 In 5-15 and In 31-42).

Mangold et al does not explicitly teach decrypting a local key using a value stored in a hidden

register. Iijima discloses a method of key security in processing data (see for example; abstract)

including using a value stored in hidden memory (col 5, In 31-35) for decrypting an encryption

key (see for example column 3, lines 39-45). One of ordinary skill in the art at the time of the

applicant's invention would have been able to replace the key exchange means of Mangold with

the key encrypting and decrypting means of Iijima within each respective first and second logical

circuits. It would have been obvious to one of ordinary skill in the art at the time of the

applicant's invention to combine the teachings of Iijima within the system of Mangold et al

because it would have improved key integrity by controlling the distributed use of the second

key. Furthermore, the Mangold-Iijima combination does not explicitly teach hidden registers.

Nally et al discloses storing of data in hidden registers so that the data is inaccessible by

software (see for example; col 14 In 34-49). It would have been obvious to one of ordinary skill

in the art at the time of the applicant's invention to combine the teachings of Nally et al within

the Mangold-Iijima combination because it would have increased security of tampering, by storing values in memory, which is harder to access.

12.   As per claim 20, Mangold-Iijima discloses the claimed limitations as described above (see claim 19). Mangold further discloses a host processor (see for example; CPU 115 fig 1); a communication link connecting said host processor to said first logical circuit and to said second logical circuit (see for example, bus 120 fig 1; processors or inherently connected to logical circuits through communication links in the setup of a computer); and memory coupled to said host processor (see for example, 108 of fig 1), said memory when run on said host processor are operable to generate a local key (see for example, session key, col 6 ln 42-55). In the Mangold-Iijima combination, one of ordinary skill in the art at the time of the applicant's invention would have realized a first and second key for each of the logical circuits, since each key is generated from a value of the each circuit.

13.   As per claim 21, Mangold-Iijima discloses the claimed limitations as described above (see claim 20). Iijima further discloses memory comprising instruction operable to access said value (see for example column 5, lines 31-41). One of ordinary skill in the art at the time of the applicant's invention using hidden registers would have realized accessing the hidden register for accessing said value.

14.   As per claim 22, Mangold-Iijima discloses the claimed limitations as described above (see claim 19). Mangold et al furthest discloses a 1394 encryptor operable to encrypt signal for transfer over an IEEE 1394 communication link (see for example; DTCP fig 1 and col 4 ln 28-56).

15.   As per claim 23, Mangold-Iijima discloses the claimed limitations as described above

(see claim 19). Mangold further discloses decrypting a broadcast signal (see for example, col 6

ln 16-30). As for decrypting an encrypted key using a value in said broadcast hidden register.

Iijima further discloses decrypting of an encrypted key using a value in stored memory (see for

example column 3, lines 39-45). As for a broadcast decryptor comprising a broadcast hidden

register and decrypting an encrypted key using a value in said broadcast hidden register.

Mangold et al discloses a broadcast decryptor (see for example; DTCP decryptor, col 6 ln 10-

15). Nally et al discloses storing of data in hidden registers so that the data is inaccessible by

software (see for example; col 14 ln 34-49). It would have been obvious to one of ordinary skill

in the art at the time of the applicant's invention to combine the teachings of Nally et al within

the Mangold-Iijima combination because it would have increased security of tampering, by

storing values in memory, which is harder to access.

16.   As per claim 24, Mangold-Iijima discloses the claimed limitations as described above

(see claim 22). Mangold further discloses memory when run on said host processor is operable

to generate a broadcast encryption key (see for example; content key, col 6 ln 3-15). As for

accessing a broadcast hidden register, and to encrypt said broadcast encryption key, Iijima

discloses means of accessing value in memory component (see for example column 5, lines 31-

41) and encrypting a broadcast encryption key (see for example column 3, lines 39-45). As for

accessing said broadcast hidden register, Nally et al discloses storing of data in hidden registers

so that the data is inaccessible by software (see for example; col 14 ln 34-49). It would have

been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine

the teachings of Nally et al within the Mangold-lijima combination because it would have

increased security of tampering, by storing values in memory, which is harder to access.

17.   Claims 2-5 and 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Ciacelli US Patent 6,236,727 in view of Dillon et al, US Patent 5,652,795

18.   As per claims 2, 4-5 and 7-9, Ciacelli discloses the claimed limitations as described

above (see claim 1) and further discloses the step of encrypting broadcast encryption key

[column 6, lines 40-41], Ciacelli does not explicitly teach accessing a value in a hidden register

on said first logical circuit. However Dillon teaches accessing a value in a hidden register on

said first logical circuit (see for example, UK Register, col 7 ln 11-25). It would have been

obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the

teachings of Dillion within the system of Ciacelli because it would have increased key security

by restricting access to a stored encryption key the. As for a value in a hidden register, the office

takes official notice that hidden registers are notoriously well known in the art to provide for

storing information un-accessible by software. It would have been obvious to one of ordinary

skill in the art at the time of the applicant's invention to use hidden registers in storing values for

encryption and decryption in system of Ciacelli because it would have increased security of

tampering, by storing values in memory, which is harder to access.

19.   As per claim 3, the combination of Ciacelli and Dillon et al discloses the claimed

limitations as describe above (see claim 2). Dillon further discloses modifying the value in said

register (see for example; col 7 ln 60-col 8 ln 4). Since keys are stored in the registers,

modification of the keys inherently modifies the registers storing the key values.

20.   Claims 12-13 and 17-18 are rejected under 35 U.S.C. 103 (a) as being unpatentable

over Iijima US Patent 5,202,922 in view of Searle, US Patent 6, 683, 954.

21.   As per claims 12, Iijima teaches the method as applied above. Furthermore, Iijima

teaches accessing a value in a non-volatile memory in said accessing a value stored in a

memory in the circuit and based upon said value encrypting said local encryption key [column 3,

lines 25-41, column 5, lines 23-31]. Iijima does not explicitly teach encrypting said local

encryption key based upon a value accessed in a register in said first logical circuit. Searle

discloses a method of encrypting an encryption key based upon a value accessed in a system

component (see for example, col 4 ln 59-col 5 ln 7). One of ordinary skill in the art at the time of

the applicant's invention would have realized a register to be the similar to the listed

components of Searle. Both Iijima et al and Searle disclose a method of key security and control

in processing digital data. It would have been obvious to one of ordinary skill in the art to

combine the teachings of Searle within the system of Iijima because it would have improved key

integrity and control by using values accessed to by some system component as a key for

encryption (see for example, Searle col 6 ln 28-31).

22.   As per claim 13, Iijima discloses the claimed limitations described above (see claim 11).

Furthermore, Iijima teaches accessing a value in a non-volatile memory in said accessing a

value stored in a memory in the circuit and based upon said value encrypting said local

encryption key [column 3, lines 25-41, column 5, lines 23-31]. Iijima does not explicitly teach

encrypting said local encryption key based upon a value accessed in a register in said first

logical circuit. Searle discloses a method of encrypting an encryption key based upon a value

accessed in a system component (see for example,, col 4 In 59-col 5 In 7). One of ordinary skill

in the art at the time of the applicant's invention would have realized a register to be the similar

to the listed memory components of Searle. Both Iijima and Searle disclose a method of key

security and control in processing digital data. It would have been obvious to one of ordinary

skill in the art to combine the teachings of Searle within the system of Iijima because it would

have improved key integrity and control by using values accessed to by some system

component as a key for encryption (see for example, Searle col 6 In 28-31).

23.   As per claim 17, Iijima discloses the claimed limitations described above (see claim 10).

Iijima does not explicitly teach polling a first hidden register in said first logical circuit. Searle

discloses a means of polling memory (see for example, checksum is determined, col 8 In 53-

61), determining whether the value has been modified (see for example col 9 In 6-17), and

stopping said processing of said digital signal if said information was modified (see for example,

col 9 In 10-17). A hidden register is a form of memory used for storing data and is similar to the

purposes of memory disclosed by Searle (see for example, ROM col 5 In 1-7). It would have

been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine

the teachings of Searle within the system of Iijima et al because it would have provided better

security towards tamper-proofing by detecting whether memory storing valuable information is

tampered or modified.

24.   As per claim 18, Iijima-Searle discloses the claimed limitations described above (see

claim 17). Searle further discloses notifying the user if information was modified (see for

example; col 7 In 61-col 8 In 2). Communications with a broadcast provider is well known in the

art. One of ordinary skill in the art at. the time of the applicant's invention would have recognized

that notification is sent by any communications means. In broadcasting, it is important for the

provider to know such modification to important information to take appropriate measures. It

would have been obvious to one of ordinary skill in the aft to send such notification to a

broadcast provider instead of a user because it would have provided important information to

the party controlling the distribution of control.

25.   Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Iijima US Patent

5,202,922 US Patent 5,202,922 in view of Blatter et al, US Patent 5,878,135.

26.   As per claim 14, Iijima discloses the claimed limitations described above (see claim 10).

Iijima does not explicitly teach said first logical circuit to modify a header in said bitstream to

indicate that said bitstrearn is encrypted. Blatter et al discloses a method of processing digital

data (see for example; abstract) including a modifying a header in said bitstream to indicate

that said bitstrearn is encrypted (see for example; encrypted indicator, col 3 In 30-35). It would

have been obvious to one of ordinary skill in the art at the time of the applicant's invention to

combine the teachings of Blatter et al within the system of Iijima because it would have provided

the option of processing non-encrypted data and encrypted data in the same system. Encrypting

data is essential in security of important data, however, different security levels exists where

certain data can be transferred in an unencrypted manner. A means for a system in determining

such encrypted and unencrypted data is necessary to provide different security level

approaches.

27.   Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Iijima US Patent 5,202,922 in view of Blatter et al, US Patent 5,878,135, as applied to claim 14 above, and further in view of Eyer et al, US Patent 5,485,577.

28.   As per claim 15, Iijima-Blatter discloses the claimed limitations described above (see claim 14). Blatter et al further discloses a command indicating a type of encryption (see for example; col 5 ln 35-54). Iijima-Blatter does not explicitly teach wherein said type is between even and odd encryption. Eyer et al discloses processing digital data (see for example; fig 1) comprising of switching between even and odd encryption (see for example col 8 ln 12-29). Eyer et al discloses the even/odd encryption type as a means of changing encryption keys (see for example, col 7 ln 46-58). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to employ the teachings of Eyer within Iijima-Blatter because it would have provided an organized method of controlling encryption keys while maintaining the security of changing encryption keys.

29.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Iijima US Patent 5,202,922 in view of Eyer et al, US Patent 5,485,577.

30.   As per claim 16, Iijima discloses the claimed limitations described above (see claim 10). Iijima does not explicitly teach, wherein said encryption key is switched between even and odd. Eyer et al discloses processing digital data (see for example; fig 1) comprising of switching between even and odd encryption (see for example col 8' ln 12-29). Eyer et al discloses the even/odd encryption type as a means of changing encryption keys (see for example, col 7 ln 46-58). It would have been obvious to one of ordinary skill in the art at the time of the applicant's

invention to combine the teachings of Eyer within Iijima because it would have provided an

organized method of controlling encryption keys while maintaining the security of changing

encryption keys.

31.   Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold et al,

US Patent 6,668,324, in view of Iijima, US Patent 5,202,922 as applied to claim 19 above, and

further in view of Eyer et al, US Patent 5,485,577.

32.   As per claim 25, Mangold-Iijima discloses the claimed limitations as described above

(see claim 19). Mangold-Iijima does not explicitly teach a plurality of hidden registers and a

control register operable to store a value to indicate which of said hidden registers is used for

encryption. Mangold discloses a means of changing keys (see for example; randomly

generated, col 6 ln 40-42). Eyer discloses a first logical circuit (see for example; col 4 ln 29-47)

including a plurality of memory banks (see for example; fig 4a and col 7 ln 59-65) and a control

message (see for example; rekey message col 8 ln 1-11) for controlling which of said memory

banks is used for encryption (see for example; col 8 ln 1-42). It would have been obvious to one

of ordinary skill in the art at the time of the applicant's invention to combine the teachings of

Eyer within the Mangold-Iijima combination because it would have increased key integrity and

provided key organization through controlling which key is to be used for encryption. As for a

plurality of hidden registers and a control register, The office takes official notice that hidden

registers are notoriously well known in the art to provide for storing information unaccessible by

software. It would have been obvious to one of ordinary skill in the art at the time of the

applicant's invention to use hidden registers in storing values for encryption and decryption in

the Mangold-Iijima combination because it would have increased security of tampering, by

storing values in memory, which is harder to access.

Response to Arguments

33.   Applicant's arguments with respect to claim 1-25 have been considered but are moot in

view of the new ground(s) of rejection.

Conclusion

34.   Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The

examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

December 21, 2004

KIM VU
SUPERVISORY PATENT EX
TECHNOLOGY CENTER